УДК 343.985

П. Л. Боровик
доцент кафедры правовой информатики
Академии МВД Республики Беларусь,
кандидат юридических наук

КОНЦЕПТУАЛЬНЫЕ ПОДХОДЫ ИНОСТРАННЫХ ГОСУДАРСТВ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализ мировых тенденций свидетельствует о том, что проблема обеспечения информационной безопасности становится одной из наиболее актуальных. Это аргументируется рядом следующих обстоятельств: в условиях глобализации реализация жизненно важных интересов личности, общества и государства осуществляется посредством процессов информатизации; информационная сфера приобрела статус системообразующей, и от нее в значительной степени зависит уровень экономического, социального, политического развития общества и государства; специфика информационной сферы такова, что негативные последствия реализации угроз информационной безопасности проявляются в других сферах жизнедеятельности личности, общества и государства и влияют на национальную безопасность в политической, экономической и иных областях; анализ существующих в мире вызовов и угроз показывает, что в современных условиях возрастает опасность совершения трансграничных преступлений, возникновения кризисных ситуаций и иных противоправных действий с применением современных информационно-коммуникационных технологий [1].

В указанных условиях особую актуальность приобретают вопросы формирования активной, согласованной информационной политики международного сообщества по противодействию информационным угрозам, защиты информационных ресурсов и коммуникаций национальных органов власти и управления. В этой связи возникает необходимость рассмотрения концептуальных подходов информационной безопасности иностранных государств, позволяющих в условиях глобализации заблаговременно выявить и нейтрализовать опасности и угрозы в информационной сфере.

Концептуальные подходы к обеспечению информационной безопасности иностранных государств опираются на государствен-

ные и международные нормативные правовые акты, регулирующие внутренние и внешние политические отношения. Ключевую роль здесь выполняют национальные стратегии информационной безопасности (кибербезопасности) — политические документы, принятые в том или ином государстве, в соответствии с которыми осуществляется политика обеспечения информационной безопасности страны. Подобного рода документы не только определяют стратегические цели, конкретную политику и регулирующие меры для достижения и поддержания высокого уровня информационной безопасности, но и имеют важное методологическое значение для системы обеспечения международной безопасности.

Первые национальные стратегии информационной безопасности начали появляться в начале предыдущего десятилетия. Одной из первых стран, в которой информационная безопасность была отмечена в качестве стратегической проблемы государственной важности, стали Соединенные Штаты Америки. В результате в 2003 году в США принята первая Национальная стратегия безопасности в киберпространстве, являющаяся частью более общей Стратегии обеспечения национальной безопасности. В последующем основным концептуальным документом в системе обеспечения информационной безопасности США стала Международная стратегия по действиям в киберпространстве, подписанная в 2011 году.

Подобные планы мероприятий и стратегии в свое время были приняты и в большинстве стран Европейского союза (ЕС). Так, начиная с 2006 года вопросам обеспечения информационной безопасности на государственном уровне уделяется внимание в Швеции, Эстонии, Словакии, Финляндии, Голландии, Чехии, Германии, Франции, Великобритании и других странах.

Детальное изучение содержания стратегий информационной безопасности большинства иностранных государств показало, что каждая из них формирует собственную модель решения задачи защиты информации от внутренних и внешних угроз. Как правило, в стратегиях предусматривается административный механизм, позволяющий частным и государственным заинтересованным сторонам формировать политику информационной безопасности; определяются цели и способы развития государственных возможностей и необходимой законодательной базы для противодействия преступлениям против информационной безопасности; обосновывает-

ся значимость разработки образовательных программ в сфере информационной безопасности; отмечается важность международного сотрудничества как со странами — членами ЕС, так и со странами, не входящими в ЕС; аргументируется необходимость проведения комплексных исследований, направленных на разрешение проблемы информационной безопасности и отказоустойчивости различного рода информационных систем и сервисов и др.

Вместе с тем результаты анализа содержания стратегий информационной безопасности иностранных государств свидетельствуют об отсутствии единых подходов к пониманию сущности и определению содержания категории «информационная безопасность» («кибербезопасность»), а также ряда иных ключевых терминов, необходимых как для теоретического осмысления информационной безопасности, так и для выработки и проведения политики в этой области. Соответственно, интерпретация проблем, связанных с информационной безопасностью, также существенно различается, что отражается на понятийно-категориальном аппарате, используемом в данной сфере. Как следствие, различаются и подходы к составлению стратегий, что приводит к невозможности сформулировать общие цели для международного сообщества по обеспечению информационной безопасности на глобальном уровне.

Наряду с отсутствием единого терминологического аппарата и согласованного подхода к реализации политики международной информационной безопасности, в действующих стратегиях не указываются и конкретные планы действий в случае обнаружения угроз, что не только усложняет процесс международного сотрудничества в данной сфере, но и приводит к невозможности выработать соответствующие практические рекомендации по реализации поставленных целей и задач для правительственных ведомств, национальных органов власти и других государственных органов.

Из этого ясно, что в современных условиях национальные стратегии обеспечения информационной безопасности иностранных государств уже не в состоянии в полной мере выполнять задачи, которые ставились при их создании.

Основываясь на результатах проведенного исследования, можно утверждать, что в современных условиях необходим единый и комплексный механизм обеспечения информационной безопасности на глобальном уровне. Первым шагом на пути к реализации

этой задачи может стать принятие в рамках ООН и Совета Европы единого международного договорного правового акта. Для его реализации необходимы: проработка и уточнение содержательного наполнения понятийно-категориального аппарата и его последующая унификация; гармонизация законодательной базы в каждом отдельно взятом государстве; определение механизмов своевременного реагирования на угрозы информационной безопасности, разработка конкретных планов действий, четкое указание их целей и спектра решаемых проблем; проведение совместных учебных мероприятий (учений, тренингов, семинаров и др.). Совершенно очевидно, что решение этой задачи требует координации усилий, согласованного сотрудничества и партнерства на всех уровнях: частном, корпоративном, национальном и международном.

Список основных источников

1. Концептуальные подходы к разработке проекта Рекомендаций по совершенствованию и гармонизации национального законодательства государств — участников СНГ в сфере обеспечения информационной безопасности [Электронный ресурс] / Региональное содружество в области связи. — Режим доступа: www.rcc.org.ru/...e.../5_2_Konceptualnie_podhody_k_inform_bezopasnosti.doc. — Дата доступа: 03.10.2017.

УДК 343.236

О. В. Ермакова

доцент кафедры уголовного права и криминологии
Барнаульского юридического института МВД России,
кандидат юридических наук, доцент

ВОПРОСЫ ОПРЕДЕЛЕНИЯ МОМЕНТА ОКОНЧАНИЯ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ (ст. 159.6 УК РФ)

Общий состав мошенничества (ст. 159 УК РФ), а также его специальные виды (ст. 159.1–159.6 УК РФ) сконструированы по типу материального состава. Данный вывод основывается на том положении, что все виды мошенничества принадлежат к числу хи-